AMENDMENT TO THE SPECIFICATION

Page 1, below the title of the invention, please add the following:

-- BACKGROUND --

Page 6, after the second full paragraph, please add the following:

-- SUMMARY --

Page 6, please amend the third full paragraph as follows:

The invention is based on the problem of providing a method for protecting data that has increased security compared to prior art methods.

Page 6, please amend the sixth full paragraph as follow:

These problems are solved by the features described herein.

Page 7, please amend the last bullet point as follows:

- In an advantageous embodiment, RA attacks are prevented by the biometric feature not being read into an external reader. In another advantageous embodiment presupposing external readers, RA attacks are impeded compared to the prior art since the method rejects two exactly identical digital representations of the biometric feature.

Page 8, please amend paragraph one as follows:

In one advantageous embodiment of an initialization phase (enrolment) to the authentication phase of the method according to the application, in one step the relevant biometric feature is accordingly digitized. In a further step, secret data are provided. In case of a public-key method the key generation necessary for an asymmetric signature method, i.e. the generation of a signature key, is effected. In a further step, the secret data are coded fault-tolerantly on the basis of a coding-theory method and encrypted on the basis of the biometric feature.

Page 8, please amend paragraph two as follows:

In another advantageous embodiment of the initialization phase, the secret data are first coded fault-tolerantly. The resulting code word is longer than the original message; the redundant information serves to decode a message in which some bits are flipped. The code word then is encrypted on the basis of the biometric feature.

Page 8, please amend paragraph three as follows:

In another advantageous embodiment, the code word is generated by the secret data being multiplied with a generating matrix. This is for example an efficient method for representing the space of allowed code words.

Page 8, please amend paragraph four as follows:

In another variant of the initialization phase, the secret data (message) are not changed by the coding. Instead, separate correction data are created. Said data describe the space of allowed code words.

Page 8, please amend paragraph five as follows:

In another advantageous embodiment of the authentication phase, the encrypted code word is first decrypted on the basis of the biometric feature. The encryption method is to have the property that single flipped bits have no influence on other bits. A suitable encryption method is the application of the bit-by-bit exclusiveOR rule (XOR).

Page 8, please amend paragraph six as follows:

In a further variant of the initialization phase, separate correction data are created in dependence on the biometric feature.

Page 8, please amend paragraph seven as follows:

In another a variant of the authentication phase, separate correction data are first created in dependence on the biometric feature. In a further step, the biometric feature measured in the initialization phase is recovered. This is done on the basis of said correction data, i.e. the correction data created in the initialization phase and the biometric feature measured in the authentication phase. In a further step, the secret data are decrypted on the basis of the recovered biometric feature data.

Page 9, please amend paragraph one as follows:

In another embodiment, the correction data are created by calculation of parameters obtained from the biometric feature modulo n. On the basis of said data, values whose deviation from the true value is smaller than or equal to n are mapped onto the true value, while values whose deviation is greater than n are mapped onto a random value.

Page 9, please amend paragraph two as follows:

In another embodiment, the authentication correction data are created and calculation of parameters obtained from the biometric authentication feature modulo n. The biometric feature data are recovered by determining the difference of the residues. This is exactly the difference of the values when the deviation is smaller than n.

Page 9, please amend paragraph three as follows:

In another embodiment, the correction method is user-specific. This permits the correction capacity to be adapted to the variance of the biometric features within a user.

Page 9, please amend paragraph four as follows:

In another embodiment the digitized feature is additionally broken down into a public and a nonpublic or secret part within the second step for providing a possibility of quantifying the effort of brute-force attacks and thus, if the system is suitably designed, a general quantification of the system with respect to protection by biometry. Since only the nonpublic part of the biometric feature is used for coding the signature key, the effort for a brute-force attack remains quantifiable.

Page 9, please amend paragraph five as follows:

In another embodiment, empirical inquiries are preferably used for breaking down the digitized biometric feature data since they are most easily performed at present.

Page 9, please amend paragraph six as follows:

In another embodiment, a hash value is preferably created with the aid of a hash function from the digitized biometric feature data or from the nonpublic portion thereof for coding the private key or signature key. This has the advantage of reducing the feature data to a fixed-length bit string and thus also simplifying the coding of the affiliated signature key, which can then be easily performed with an XOR operation for example.

Page 10, please amend paragraph one as follows:

In another embodiment, a hash value is still preferably created with the

aid of a hash function from the digitized biometric feature data created in the authentication phase, said value being compared with already stored hash values of preceding authentications. Since the hash function is a special form of so-called one-way functions, it has the property of collision freedom. The term collision freedom is understood in cryptography to mean that similar but not identical texts are to yield completely different check sums. Each bit of the text must influence the check sum. This means, in simplified terms, that the function always yields exactly one identical output value of fixed bit length in case of identical input values. This property is exploited by the method according to the application, since it is virtually impossible to obtain exactly two identical measuring data records when the same biometric feature is repeatedly captured, as mentioned above. If comparison between the current and the stored hash values therefore leads to a positive result, this is a strong indication of the possibility that a replay attack is involved. Security can accordingly be guaranteed by aborting authentication.

Page 10, please amend paragraph two as follows:

The biometric features to be used for the method in question are preferably behavioral biometrics. These have the advantage of being difficult to imitate. Simple copying of patterns or features is virtually excluded.

Page 10, please amend paragraph three as follows:

In another embodiment, the method according to the application uses the handwritten signature as the behavioral biometric since it can be easily broken down into dynamic and static portions, which in turn serve to break down the biometric feature into secret and public parts.

Page 10, please amend paragraph four as follows:

In another embodiment, the handwritten signature is preferably broken down into a public and a secret part such that the secret part of the signature is a proper subset of the dynamic information, thereby making quantification possible or keeping it possible.

Page 10, please amend paragraph five as follows:

In another embodiment, the biometric feature in question is measured and digitized several times in order to improve the fault-tolerance or determination of variance of the biometric feature data when they are digitally captured.

Page 10, please amend paragraph six as follows:

In another embodiment, a conventional public-key method is preferably proposed for key generation since it is widespread and works reliably.

Page 11, please amend paragraph one as follows:

An apparatus is proposed for carrying out the method according to the application in a simple way.

Page 11, after the second paragraph , please add the following:

-- BRIEF DESCRIPTION OF THE DRAWINGS --

Page 11, please amend paragraph 3 as follows:

Further features and advantages of the invention can be found in the following description of an example with reference to the drawing, in which:

Page 12, after the third paragraph, please add the following:

-- DETAILED DESCRIPTION--